UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/798,079	03/11/2004	Aaron Charles Newman	AS2	5342

31097 7590 11/18/2010

PETER S. CANELIAS
LAW OFFICES OF PETER S. CANELIAS
420 LEXINGTON AVENUE
SUITE 2620
NEW YORK, NY 10170

EXAMINER	
KIM, PAUL	
ART UNIT	**PAPER NUMBER**
2169	

MAIL DATE	DELIVERY MODE
11/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/798,079	NEWMAN ET AL.	
	Examiner	Art Unit	
	PAUL KIM	2169	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 September 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *98-104* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *98-104* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is responsive to the following communication: Amendment filed on 16 September 2010.

2. Claims 98-104 are pending and present for examination.

Response to Amendment

3. Claim 98 has been amended.

4. No claims have been further cancelled.

5. No claims have been newly added.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 98 and 101** are rejected under 35 U.S.C. 103(a) as being unpatentable over Bapat et al, U.S. Patent No. 6,038,563 (hereinafter referred to as BAPAT), filed on 25 March 1998, and issued on 14 March 2000, in view of Glasser et al, U.S. Patent No. 5,956,715 (hereinafter referred to as Glasser), filed on 23 September 1996, and issued on 21 September 21 1999, and in further view of Belfiore et al, U.S. Patent No. 6,990,513 (hereinafter referred to as Belfiore), filed on 22 June 2001, and issued on 24 January 2006.

8. **As per independent claim 98,** BAPAT, in combination with Glasser and Belfiore, discloses:

> A computer readable medium having code to perform a computer implemented method for protecting a database hosted on a server, comprising:

installing a console on a remote computer system for monitoring activity on the database {See BAPAT, C4:L58-65, wherein this reads over "a network management system 100 having an access control engine (ACE) 102 that restricts access by initiators (e.g., users, and application programs acting on behalf of users) to the managed objects in a network"}, the remote computer system having a first tangible computer readable medium {See GLASSER, C6:L17-20, wherein this reads over "Client 130 can include a floppy disk drive or other persistent storage device"};

presenting the installed console through a user interface {See GLASSER, C5:L13-16, wherein this reads over "a user interface component 180, which is used in accessing a file or folder on hard disk 121 remotely from another node of network 110"};

the user interface being displayed on a monitor {See GLASSER, C5:L13-16, wherein this reads over "a user interface component 180, which is used in accessing a file or folder on hard disk 121 remotely from another node of network 110"};

registering a listener agent with the console {See BAPAT, C5:L44, wherein this reads over "user information, identifying the request initiator"; C9:L46-61, wherein this reads over "access rules are defined in terms of access rights of groups"}, the server having a second tangible compute readable medium {See BAPAT, C7:L37-38, wherein this reads over "memory 164, including both volatile high speed RAM and non-volatile storage such as magnetic disk storage"};

the listener agent being installed on the server hosting the database {See BAPAT, C8:L18-29, wherein this reads over "The MIS 150 and auxiliary servers 152, 154 all maintain identical copies of a library of access control procedures as well as a copy of the access control object tree"};

establishing a secure connection between the console and the listener agent {See BAPAT, C4:L58-65, wherein this reads over "a network management system 100 having an access control engine (ACE) 102 that restricts access by initiators (e.g., users, and application programs acting on behalf of users) to the managed objects in a network"} wherein the secure connection operates over a secure socket layer and the console and the listener agent are in cross-platform communication using simple object access protocol {See Belfiore, C26:L20-44, wherein this reads over "a SOAP-based message representation"; and C27:L1-5, wherein this reads over "the standard HTTP security mechanism (SSL) can be used by the message component"};

the console and the listening agent monitoring activity at an application level of the database {See BAPAT, C4:L58-65, wherein this reads over "a network management system 100 having an access control engine (ACE) 102 that restricts access by initiators (e.g., users, and application programs acting on behalf of users) to the managed objects in a network"};

configuring the listener agent with a first set of rules having a set of security attributes {See BAPAT, C17:L3-14, wherein this reads over "[t]his filter 291 passes "access grant" and "access denial" event notifications generated by the MIS"};

installing a collector agent to be in communication with the listener agent for collecting a plurality of database events {See BAPAT, C17:L3-14, wherein this reads over "[t]his filter 291 passes "access grant" and "access denial" event notifications generated by the MIS"} wherein the collector agent includes a plurality of collector definitions, each one of the collector definitions being associated with a database instance {See Bapat, C14:L66-C15:L5, wherein this reads over "a set of filters in the log server determine which event notifications are stored"};

deconstructing the plurality of database events into a plurality of atomic messages {See BAPAT, C18:L24-27, wherein this reads over "[u]ser queries requesting information from tables to which the user does not have access rights are rejected by the SQL engine"};

analyzing the plurality of atomic messages for compliance with the first set of rules {See BAPAT, C17:L15-19, wherein this reads over "a Security Alarm log 293 that is separate from the security audit trail 192, where security alarms are generated and stored in the log only when there is a denial of object access"};

executing compliant database events {See BAPAT, C18:L19-27, wherein this reads over "only queries in full compliance with those access rights are processed"; and C28:L31-37, wherein this reads over "[a]ccess is allowed only for the objects to which the user has appropriate access rights"};

transmitting a signal to a console operator when a database event is not compliant with the first set of rules {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}, wherein transmitting the signal to the console includes using a dispatcher agent connected to the console {See Bapat, Figure 5, an "Access Control Decision Function"} over a peer-to-peer channel {See Bapat, Figure 8, wherein the MIS transmits event notification messages to specific users and entities} and transmission of the signal is platform independent {See Bapat, col. 4, lines 58-65, wherein this reads over "the network can be virtually any type of computer implemented network that uses a management protocol for performing management functions"};

allowing a console operator to create exceptions to the first set of rules when signals are sent by the listener agent {See BAPAT, C11:L39-51, wherein this reads over "users authorized to modify the access control tree"};

updating the first set of rules with the exceptions created by the console operator {See BAPAT, C11:L39-51, wherein this reads over "users authorized to modify the access control tree"};

storing the signals received by the console operator in a data file residing with the console {See BAPAT, C12:L56-57, wherein this reads over "[t]he deny/grant decision for each access request may be stored in a security audit trail"}, in association with the second tangible computer readable medium.

While BAPAT may fail to expressly disclose the features related to the recited remote computer system, GLASSER discloses a system for controlling user access to a network server wherein the client components include a persistent storage device and a user interface component for connecting with the network server. Wherein BAPAT discloses a managed information object system wherein users connect and access data via an access control server, it would have been obvious to one of ordinary skill in the art to modify said invention with that disclosed by GLASSER such that a client may utilize a user interface to communicate with the access control server.

One of ordinary skill in the art would have been motivated to make the aforementioned modification such that the client may remotely access and monitor activity on the database of an access server.

9. **As per independent claim 101,** BAPAT, in combination with GLASSER and BELFIORE, discloses:

> The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 98, wherein the step of analyzing further comprises the steps of:
>
> determining whether an executable SQL statement contains a write operation to a data dictionary {See BAPAT, C6:L4-11, wherein this reads over "[i]f a suspicious directory name is found 68, the control function is notified"};
>
> preventing the data dictionary from being written to {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}.

10. **Claim 99** is rejected under 35 U.S.C. 103(a) as being unpatentable over BAPAT as applied to claims 89 and 90, in view of GLASSER and BELFIORE, and further in view of Shostack et al (U.S. Patent No. 6,298,445, hereinafter referred to as SHOSTACK), filed on 30 April 1998, and issued on 2 October 2001.

11. **As per dependent claim 99,** BAPAT, in combination with GLASSER, BELFIORE and SHOSTACK, discloses:

> The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 98, wherein the step of analyzing further comprises the steps of:
>
> determining whether the plurality of atomic database events include an executable SQL statement that exploits a buffer overflow vulnerability in the database {See SHOSTACK, Table 1, wherein this reads over "Check for known bugs in the servers . . that are vulnerable to buffer overflow attacks" and "X-windows. Check for open permissions that allow snooping of remote X session, unpatched libraries and executables vulnerable to buffer overflow attacks"};
>
> preventing the executable SQL statement from executing {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}.

While BAPAT fails to expressly disclose a method of "processing the plurality of database events by detecting whether an executable SQL statement exploits a buffer overflow vulnerability in the

database," SHOSTACK discloses a method of check for buffer overflow vulnerabilities. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT and GLASSER by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

12. **Claim 100** is rejected under 35 U.S.C. 103(a) as being unpatentable over BAPAT as applied to claims 89 and 90, in view of GLASSER and BELFIORE, and further in view of Reshef et al (U.S. Patent No. 6,321,337, hereinafter referred to as RESHEF), filed on 9 September 1998, and issued on 20 November 2001.

13. **As per dependent claim 100,** BAPAT, in combination with GLASSER, BELFIORE, and RESHEF, discloses:

> The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 98, wherein the step of analyzing futher comprises the steps of:
>
> detecting whether an executable SQL statement includes an operating system call {See RESHEF, C10:L 21-35, wherein this reads over "[a]ny breach of the permitted flow sequences by disorderly operating system calls or looping will be trapped and logged"};
>
> preventing the executable SQL statement from making the operating system call {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}.

While BAPAT fails to expressly disclose a method of "detecting an executable statement includes an operating system call," RESHEF discloses a method of checking for operating system calls which result in a breach of permitted flow sequences. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT and GLASSER by combining it with the invention disclosed by RESHEF.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

14. **Claims 102-104** are rejected under 35 U.S.C. 103(a) as being unpatentable over BAPAT as applied to claims 89 and 90, in view of GLASSER and BELFIORE, and further in view of Rowland (U.S. Patent No. 6,405,318, hereinafter referred to as ROWLAND), filed on 12 March 1999, and issued on 11 June 2002.

15. **As per dependent claim 102,** BAPAT, in combination with GLASSER, BELFIORE, and ROWLAND, discloses:

> The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 98, wherein the step of analyzing further comprises the steps of:
>
> determining whether an executable SQL statement alters a set of auditing configurations existing on the database {See ROWLAND, C5:L61-67, wherein this reads over "name a local directory in an odd way to hide their work"};
>
> preventing the set of auditing configurations from being altered {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}.

While BAPAT fails to expressly disclose a method "wherein said unauthorized activity is interfering with auditing settings," ROWLAND discloses a method wherein suspicious directory activity is detected {See ROWLAND, C5:L61-67}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT and GLASSER by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

16. **As per dependent claim 103,** BAPAT, in combination with GLASSER, BELFIORE, and ROWLAND, discloses:

> The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 98, wherein the step of analyzing further comprises the steps of:
>
> determining whether an executable SQL statement includes a write operation to a set of audit records existing in a log file {See ROWLAND, C6:L4-11, wherein this reads over "[t]he system checks to determine if the system audit records have been altered or are missing"};

> preventing the audit records existing in the log file from being written to {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}.

While BAPAT fails to expressly disclose a method "wherein said unauthorized activity is interfering with audit records," ROWLAND discloses a method wherein "[t]he system checks to determined if the system audit records have been altered or are missing" {See ROWLAND, C6:L4-11}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT and GLASSER by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

17. **As per dependent claim 104,** BAPAT, in combination with GLASSER, BELFIORE, and ROWLAND, discloses:

> The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 98, wherein the step of analyzing further comprises:
>
> the steps of: determining whether an executable SQL statement includes an attempt by a user to obtain administrator access by changing a configuration file in the database {See ROWLAND, C5:L53-56, wherein this reads over "[t]he system examines the rhost file and other system authentication files to determine if dangerous security modifications to the host file have occurred"};
>
> preventing the configuration file in the database from being changed {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}.

While BAPAT fails to expressly disclose a method "wherein said unauthorized activity is modifying security settings," ROWLAND discloses a method wherein "[t]he system examines the rhost file and other system authentication files to determine if dangerous security modifications to the host file have occurred" {See ROWLAND, C5:L53-56}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT and GLASSER by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

Response to Arguments

18. Applicant's arguments filed 23 April 2010 have been fully considered but they are not persuasive.

a. Rejection of claim 99 under 35 U.S.C. 103

Applicant asserts the argument that "in contrast, Applicant's console and dispatcher operate over a peer-to-peer channel where the console may update the rules with exceptions on the fly." See Amendment, page 17. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., updating rules on the fly) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Additionally, Applicant asserts the argument that Bapat fails to teach "a peer-to-peer channel." See Amendment, page 17. The Examiner respectfully disagrees. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). The Examiner notes that Glasser discloses that "a computer network links together two or more computers by a communication pathway or pathways, allowing the computers to share resources and information." See Glasser, C1:L21-30. Accordingly, it would have been obvious to one of ordinary skill in the art that a computer network would appropriately read upon the recited feature of "a peer-to-peer channel."

Accordingly, the claim rejections under 35 U.S.C. 103 are maintained.

Conclusion

19. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to PAUL KIM whose telephone number is (571)272-2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tony Mahmoudi can be reached on (571) 272-4078. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tony Mahmoudi/
Supervisory Patent Examiner, Art Unit 2169

Paul Kim
Examiner, Art Unit 2169

/pk/